IN THE CLAIMS

Claim 1 has been amended as follows:

1.   (Currently Amended)   A   method   for   variably   generating cryptographic securities, for communications, in a host device, comprising the steps of:

for cryptographically securing a communication for a first purpose, using a first signature;

for cryptographically securing a communication for a second purpose, using a second signature; and

using a cryptographic algorithm of a first type to generate said first signature and using a cryptographic algorithm of a second type to generate said second signature, said cryptographic algorithms of said first type and said second type, for a same input set, respectively generating different respective outputs; and

entering an input set into said host device for a current communication together with an entry designating whether said current communication is for said first purpose or for said second purpose and, if said current communication is for said first purpose, operating on said input set for said current communication with said cryptographic algorithm of said first type to secure said current communication with said first signature and, if said current communication is for said second purpose, operating on the same input set for said current communication with said cryptographic algorithm of said second type to secure said current communication with said second signature.

2-19. (Cancelled)

Claim 20 has been amended as follows:

20.   (Currently amended)   A method as claimed in claim 1 comprising, in a ~~read-only~~ memory of a postal security device, storing a first program that, when executed, implements said cryptographic algorithm of said first type and ~~storing~~ providing a second program that, when executed, implements said cryptographic algorithm of said second type;

> ~~upon a need for a~~ if said current communication is for said first purpose, accessing said ~~read-only~~ memory of said postal security device, from a hardware unit outside of and in communication with said postal security device, and executing said first program in said hardware unit to secure said communication for said first purpose with a first signature produced by said cryptographic algorithm of said first type; and

> ~~upon a need for a~~ if said current communication is for said second purpose, accessing said second program ~~from~~ said ~~read-only~~ memory of said postal security device from said hardware unit and, in said hardware unit, executing said second program to secure said second communication for said second purpose with a signature generated by said cryptographic algorithm of said second type.

21.   (Previously presented)   A method as claimed in claim 1 comprising generating said first signature exclusively in a first logic module that executes said cryptographic algorithm of said first type therein under control of a first implementation program; and

generating said second signature exclusively in a second logic module by executing said cryptographic algorithm of said second type therein under control of a second implementation program.

22.   (Previously presented)   A method as claimed in claim 21 comprising storing said first implementation program in said first logic module, and accessing said first implementation program from within said first logic module, and storing said second implementation program in said second logic module, and accessing said second implementation program from within said second logic module.

Claim 23 has been amended as follows:

23.   (Currently amended)   A method as claimed in claim 21 comprising storing said first and second implementation programs in a postal security module accessible by each of said first and second logic modules, and accessing said first implementation program in said postal security device from said first logic module upon a need for a if said current communication is for said first purpose and accessing said implementation program in said postal security device from said second logic module upon a need for a if said current communication is for said second purpose.

Claim 24 has been amended as follows:

24.   (Currently amended)   A method as claimed in claim 21 wherein said first host device contains a postal security device, and storing said first implementation program in a memory of said host device outside of said postal security device and storing said second implementation program in said memory of said host device outside of said postal security device, and accessing said first implementation program in said memory from said first logic module upon a need for

-4-

a if said current communication is for said first purpose and accessing said second implementation program in said memory from said second logic module upon a need for a if said current communication is for said second purpose.

Claim 25 has been amended as follows:

25.   (Currently amended)   A method as claimed in claim 1 comprising storing a plurality of algorithms selected from the group consisting of signing algorithms and hash algorithms in a read-only memory of a postal security device;

> from a logic module outside of said postal security device having access to said read-only memory, accessing a selected one of said algorithms upon a need for a if said current communication is for said first purpose and using said selected one of said algorithms as said cryptographic algorithm of said first type in said logic module to secure said communication for said first purpose; and

> from said logic module, accessing a selected different one of said algorithms from said read-only memory of said postal security device and, upon a need for a if said current communication is for said second purpose, securing said communication for said second purpose in said logic module using said selected different one of said algorithm as said cryptographic algorithm of said second type.

26.   (Previously presented)   A method as claimed in claim 1 comprising employing the RSA algorithm as said cryptographic algorithm of the first type and employing a digital signature algorithm as the cryptographic algorithm of the second type.